Streamlining/Coordinating the Security Finding Tracking Process

The Challenge

FSA/ED IT security findings are reported and tracked by a wide variety of offices and individuals, using a wide variety of tracking systems, making it difficult to establish one central, up-to-date list of all security finings and their current status (including planned corrective actions). For example, individual system security officers track findings, as do the Office of the Chief Information Officer, the Chief Financial Officer, and the FSA Chief Information Officer—all using different tracking systems (eg, ARTS, PIP). It is also difficult to establish which tracking system, if any, is the "official" tracking system.

Version control is also an issue—for example, the Inspector General routinely issues findings in several iterations—eg, draft memo, final memo—making it even more difficult to keep track of the current status. Likewise, it appears that individuals update the status of findings without coordinating these updates with "official" tracking systems.

Finally, there is a certain "art" to extracting the exact security finding from Inspector General memos, reports, etc.

All these factors make it very challenging to accurately track both the (1) number and exact nature of IT security findings and (2) the current status of those findings, and completed or planned corrective actions to address those findings.

NOTE: It is understood that the soon-to-be-released Performance Improvement Portal (PIP) might serve as such a centralized, streamlined reporting and tracking mechanism, but is imperative that the PIP include all sources of findings if it is to meet its stated goal.

The BearingPoint Solution

BearingPoint proposes to streamline the finding-tracking process by:

1. Conducting an extensive interview/inventory process to firmly establish the individuals and offices that currently track findings—including the tools they use. This process will include the following procedures:
    a. Personal interviews
    b. Review of pertinent requirements and policies
    c. Review of existing tracking systems
    d. Review of current reporting requirements (frequency, content, format, etc.)
2. Creating a detailed "as-is/current-state" diagram
3. Conducting focus groups with key personnel to verify current reporting procedures and identify areas of improvement

4. Creating a proposed "future-state" diagram, with supporting documentation
5. If necessary or desirable, creating standardized reporting templates
6. Presenting the future state to key decisionmakers
7. If appropriate, lobby for its passage
8. If passed:
    a. Write new policy
    b. If necessary, create new tracking system
9. Conduct training on using the new system and templates
10. Conduct both an initial outreach campaign to "advertise" the new system, as well as refresher material

Note: Even if a new system is not implemented, an understanding of how all the current different tracking systems relate to one another will be of significant benefit.

Deliverables

- As-Is/Current State Diagram, with accompanying narrative
- Analysis of focus group results
- Future State Diagram, with accompanying narrative
- Lobbying materials (memos, presentations, etc.)
- New policy document outlining new tracking procedures
- Training materials
- Outreach materials (newsletter articles, emails, lobby marquee slides, etc.)

NOTE: It may or may not be necessary to create the physical tracking system itself, depending on the needs. We will leverage existing systems wherever possible.

Toolkit Audience

- OCIO
- CFO
- IG
- SSOs
- IT security contractors
- System managers

Affected Parties

The following parties will need to either be involved with, or kept abreast of, toolkit development:

- FSA security and privacy personnel involved with tracking and responding to findings
- ED OCIO staff
- FSA CFO staff
- FSA CIO staff
- Any other key personnel responsible for tracking IT security findings

Benefits

- More accurate, responsive, and timely reporting to OMB
- Increased understanding of the status and nature of IT security findings
- Greatly streamlined process for tracking security findings—significant time savings
- Elimination of duplication of effort

Assumptions

- BearingPoint will have access to key personnel
- BearingPoint will have access to key information/systems (or at least, a description of them)
- Key personnel, if they "buy in" to the concept, will be able to influence a change in procedure

Project Schedule/Resources

A project plan with milestones and delivery dates will be provided after project approval.

It should be noted that this project will require significant hours, as well as significant access to key personnel.